containing data representing at least one of: key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data and authentication data;

comparing, by the subscriber, the updated security key manifest to the pre-existing credential set containing at least one of: key size data, cryptographic algorithm designation data, key attribute data and key usage data for; and

updating, by the subscriber, the pre-existing credential set based on the comparison by generating at least one new key for the subscriber based on content of the configurable security key manifest.

39. (Amended) The apparatus of claim 36 including a trusted key manifest generator operatively responsive to digitally sign the configured security key manifest.

REMARKS

Applicant respectfully traverses and requests reconsideration.

Claims 1, 25 and 44 stand rejected under 35 U.S.C. § 112 as allegedly having insufficient antecedent basis of the limitation in the claims. Applicant has amended claim 1 to correct the typographical error and notes that with respect to claims 25 and 44, the claim recites the key attribute data is received and contained in the configured security key manifest. Accordingly, Applicant is uncertain as to why there is insufficient antecedent basis.

Claim 29 stands rejected under 35 U.S.C. § 112, 2nd paragraph as allegedly being indefinite. Applicant has amended claim 39 to correct the typographical error.

The above limitations were made to correct typographical errors and are not believed to narrow the scope of the claims. However, if the Examiner is of a different opinion, Applicant respectfully requests notification of the same in writing.

Claims 1-3, 5-10, 13-15, 18-20, 22-25, 27-31, 34-36, 38, 40, 42-44, 46 and 48 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,495,533 (Linehan). Linehan is directed to a personal key archive computing system that includes an automated

management system for managing keys to encrypt and decrypt stored data on the computing system. An authentication server authenticates a user and in response to the user accessing the computing system, the authentication server provides the user with a ticket validating the user. The client (user's computer) when creating a data file, invokes the key generator located in a separate server, or for example with the authentication server, to generate a key corresponding to a data file to be encrypted. The file based key is provided by the key server and a client uses the key to encrypt the data file which is stored in encrypted data file memory. The client application sends the ticket and data file identification to the key server. The key server checks the ticket and sends the key corresponding to the data file to the key client. The key client uses the key to decrypt the encrypted data file. The ticket can contain a key to encrypt messages sent between a client server and a key client. The personal key server generates and contains the key generator. In addition, the key server includes a key database. One control key is used for multiple files and a new control key is generated for a group of files. The control keys are used to encrypt file encryption keys which are random numbers. The control keys are generated by and kept entirely within the personal key server.

Each data file is encrypted by the client, on the user's computer, using a randomly chosen key generated by the personal key server at the time the file is created. The Linehan reference also teaches that "the size of the personal key database entries is fixed, since they contain only the control key and perhaps a few other cryptographic variables. Furthermore, existing entries in the personal key database are never updated; the only changes are the appending and new entries to the end of the personal key database." (Col. 12, lines 12-17). Hence, Linehan teaches an opposite approach to Applicant's claimed invention. Linehan does not teach or suggest an apparatus or method that provides a configurable security key manifest that contains a non-prespecified number of security keys nor dynamically controlling, through a configured key security manifest, the generation of a new security key in addition to a preexisting cryptographic security key for subscriber based on key attribute data contained in the configured security key manifest as claimed.

For example, as to claim 1, 15, 25, 36 and 44, the Office Action recites Col. 7, lines 39-45 of Linehan and equates the personal key database of Linehan to the claimed security key manifest. In particular, the Office Action indicates that the personal key database contains an

entry for each file that is to be accessed and hence is allegedly the claimed security key manifest. Applicant respectfully traverses.

Applicant respectfully submits that the personal key database of Linehan is merely a database containing control keys created by the personal key server. The personal key server only generates control keys in response to the user sending its ticket and data file identification to the key server. The personal key database is an output of the generation of a security key for each file that is supposed to be encrypted and does not control whether to generate a new security key for a subscriber based on data contained within the personal key database. To the contrary, the personal key database of Linehan is merely a database containing already generated keys that are generated by the separate key server and Linehan does not teach or suggest analyzing its personal key database to generate a new security key for the subscriber based on key attribute data contained within the personal key database. Applicant claims, among other things, generating a new security key in a dynamically controlled manner through a configured security key manifest based on key attribute data contained in the configured security key manifest. As such, these claims are believed to be in condition for allowance.

In addition, the rejection does not appear to indicate which element in the Linehan reference dynamically controls through a configured security key manifest, the generation of the new security key for the subscriber based on received key attribute data contained in the configured security key manifest. Hence, Applicant respectfully requests a showing as to which element in Linehan allegedly anticipates such a structure and operation.

In addition, claim 15 more specifically requires that the subscriber compare that data security key manifest to preexisting credential sets that contain specific information such as, but not limited to, key size data, and key usage data and also requires that the subscriber update the preexisting credential set based on the comparison by generating at least one new key based on the content of the configurable key manifest. Linehan teaches an opposite approach in that the client does not do any key generation. Instead, Linehan requires that a separate personal key server generate the key and then send the key to the subscriber. Accordingly, Linehan teaches an opposite approach to that claimed by Applicant. These differences and combinations of the noted differences above are also believed to render this claim allowable.

With respect to claims 5, 35, 38 and 48, the Office Action alleges that Linehan teaches the claimed configured security key manifest in Col. 5, lines 9-16. However, Applicant respectfully notes that the cited portion of Linehan does not describe or relate to a configured security key manifest nor does it describe such a manifest including at least one of security key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data and authentication data. To the contrary, the cited portion teaches merely that a client sends a ticket and data file identification to a server, namely, the key server and the key server checks the ticket to verify that the accessing user is permitted to access the data file and then the key server sends the key corresponding to the data file to the client so that the client can decrypt the encrypted data file since it is the client that sends the ticket and data file identification data to the key server in Linehan. In contrast, Applicant claims that an already configured security key manifest includes updated data that is contained in the configured security key manifest, since the Office Action states as to claim 1 that the personal key data base of Linehan has been equated to the claimed configurable security key manifest of Applicant's claimed invention. However, the cited portion of Linehan indicates that a subscriber sends the identification idea to a key server. However, the personal key database of Linehan is already contained in the key server. Accordingly, these claims are also believed to be in condition for allowance.

As to claims 6, 10, 20 and 31, Applicant notes that these claims require, among other things, updating the preexisting credential set based on a comparison of preexisting credential sets containing at least one preexisting cryptographic security key. Applicant again respectfully notes that Linehan actually teaches that the personal key database entries are fixed and that "personal key database are never updated". (Col. 12, line 15). Linehan in fact teaches an opposite approach to Applicant's claimed invention and teaches that the personal key database of Linehan (which Applicant respectfully challenges is not equivalent to the client security key manifest), is not updated. Applicant claims updating the preexisting credential set based on the comparison. Accordingly, these claims are also believed to be in condition for allowance.

Referring to claim 7, Applicant respectfully notes that the cited portion of Linehan merely teaches that the client or subscriber may generate a final encryption key. It is then sent to the personal key server at the time the file is created but notes that there is a disadvantage to this

variance. In contrast, Applicant claims generating a new public key pair for the subscriber based on the contents of the configurable security key manifest. Applicant is unable to find reference to the generation of such a public key pair based on a configurable security key manifest as claimed. As noted above, the configurable security key manifest is a mechanism, such as a graphic user interface or other mechanism, that allows a security officer or other operator to configure the security key manifest to facilitate key generation. Such a system is not taught or suggested by Linehan.

As to claims 8, 18 and 29, this claim requires, among other things, continuously analyzing the configured security key manifest content, prior to using a security key pair to determine whether the suitable security key is necessary for a given operation. Such an operation is not described by Linehan.

With respect to claims 9, 19 and 30, Linehan is alleged to disclose encrypting a configurable key manifest with a key and userid, and validating the userid, in an authentication ticket against userid contained in the database, citing (Col. 16, lines 13-7). However, the claims require that the key manifest be digitally signed and it must be received and analyzed as claimed. The cited portion of Linehan refers to the encrypted file and not to a digitally signed key manifest.

Referring to claims 13, 23 and 34, Linehan has been cited as allegedly disclosing using symmetric data encryption keys that are stored in a configurable security key manifest. Applicant respectfully reasserts the relevant remarks made above with respect to claim 1 and submits that these claims are also in condition for allowance.

Referring to claims 27, 28, 42 and 43, the Applicant respectfully reasserts the relevant remarks made with respect to claim 25. Accordingly, these claims are also believed to be in condition for allowance.

Claims 4, 16, 37 and 47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Linehan, in view of U.S. Publication No. 2001/0003828 (Peterson). These claims, require, among other things, issuing a configured key manifest for push based or pull based access by the subscriber, wherein the configurable security key manifest contains a non prespecified number of

security keys and wherein a configured security key manifest dynamically controls the generation of a new security key for the subscriber based on received key attribute data contained in the configured security key manifest. Applicant respectfully reasserts the relevant remarks made above with respect to the Linehan reference and further notes that the Peterson reference is directed to a client side system for scheduling and delivering web content. The Office Action cites paragraph 46 of Peterson which merely indicates that a delivery of an index and web content can be done using pull based or push based architectures. Applicant respectfully submits that the Peterson reference does not appear to be directed to the problem faced by Applicant nor to the problem faced by Linehan and is not properly combinable with the Linehan reference since Peterson appears to be silent as to a method for creating security keys. As such, this combination of references cannot render Applicant's claim obvious.

Claims 11, 12, 17, 21, 22, 26, 32, 33, 41 and 45 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Linehan, in view of U.S. Patent No. 6,230,269 (Spies). Applicant respectfully reasserts the relevant remarks made above with respect to the Linehan reference and further notes that this claim requires a generation of key pairs and dynamically controlling the number of key pairs for a subscriber in response to the content of the configured security key manifest. As such, these claims are also believed to be in condition for allowance. Moreover, the cited portion of the Spies reference (Col. 1, lines 44-50) merely indicates that authentication is achieved through cryptographic public key systems. However, as noted above, none of the cited references describe using configurable key manifests and comparing key manifests to one another and using the key manifests to generate public keys. Accordingly, these claims are also believed to be in condition for allowance.

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned "Version with markings to show changes made."

Accordingly, Applicant respectfully submits that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

By: _____
Christopher J. Reckamp
Registration No. 34,414

Date: January 13, 2003

VEDDER, PRICE, KAUFMAN &
KAMMHOLZ
222 N. LaSalle Street
Chicago, IL 60601
(312) 609-7500
FAX: (312) 609-5005

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Specification:

Please substitute the following paragraph for the current paragraph beginning at line 21, page 4.

Briefly, an apparatus and method for dynamically creating security keys for a subscriber, having at least one pre-existing security credential set, allows the configuration for N key pairs or N keys (where the cryptographic system is a symmetric key system). Such a system provides flexibility in assigning cryptographic algorithms and cryptographic keys to facilitate a change in algorithm without requiring reinitialization of a processing unit or subscriber. In addition, there can be a change in signing algorithm from message to message, for example. The apparatus and method provides a configurable security key manifest, such as a template or table, operative to contain a non-prespecified number of security keys. A security officer or other source may input key configuration data [to] through a graphic user interface template or other suitable mechanism to configure the security key manifest. Once configured (populated), the apparatus dynamically controls the generation of at least one new security key for the subscriber based on received key attribute data and based on the differences in current and prior security key manifests.

In the claims:

Please amend claims 1, 15 and 39 as follows:

1. (Amended) A method for dynamically creating security keys for a subscriber having at least one preexisting security credential set having at least one pre-existing cryptographic security key, comprising the steps of:

providing a configurable security key manifest operative to contain a non-prespecified number of security keys; and

dynamically controlling, through a configured security key manifest, the generation of at least one new security key for [a] the subscriber based on [the] received key attribute data contained in the configured security key manifest.

15. (Amended) A method for dynamically creating security keys for a subscriber having at least one preexisting security credential set having at least one pre-existing cryptographic security key, comprising the steps of:

providing a configurable security key manifest [(table)] operative to contain a non-prespecified number of security keys;

receiving, in response to providing the configurable security key manifest, data representing desired new key attribute data by presenting a configurable security key manifest template and receiving new key attribute data through the configurable security key manifest template;

dynamically controlling, through a configured security key manifest, the generation of at least one new security key for a subscriber based on the received key attribute data, wherein the configured security key manifest is an updated security key manifest containing data representing at least one of: key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data and authentication data;

comparing, by the subscriber, the updated security key manifest to the pre-existing credential set containing at least one of: key size data, cryptographic algorithm designation data, key attribute data and key usage data for; and

updating, by the subscriber, the pre-existing credential set based on the comparison by generating at least one new key for the subscriber based on content of the configurable security key manifest.

39. (Amended) The apparatus of claim 36 including a trusted key manifest generator operatively responsive to digitally sign the configured security key manifest [by;].